ELSEVIER

Discrete Applied Mathematics 111 (2001) 37–53

DISCRETE APPLIED MATHEMATICS

Two classes of ternary codes and their weight distributions

Cunsheng Ding[a,] *, Torleiv Kløve[b], Francesco Sica[a]

[a] Department of Computer Science, National University of Singapore, Block S16, Level 5, Room 05-08, 3 Science Drive 2, Singapore 117543, Singapore

[b] Department of Informatics, University of Bergen, HIB, N-5020 Bergen, Norway

Received 21 September 1999; revised 1 February 2000; accepted 13 July 2000

Abstract

In this paper, we describe two classes of ternary codes, determine their minimum weight and weight distribution, and prove their properties. We also present four classes of 1-designs that are based on the classes of ternary codes. One class of codes described here improves the existing class of ternary codes described by Ding et al. (IEEE Trans. Inform. Theory 46 (2000)).

Keywords: Group character codes; Ternary codes; Designs

1. Introduction

Ternary codes have been studied by many authors, see, for example, Bogdanova and Boukliev [1], Hamada et al. [4], van Eupen [10,11], and van Eupen and van Lint [12]. Much of the study was concentrated on ternary codes of small dimensions.

A class of $[2^n, \sum_{i=0}^{r}\binom{n}{i}, 2^{n-r}]$ group character codes $C_q(r,n)$ over GF(q), where q is odd, is described and analyzed by Ding et al. [2]. This class of codes contains the ternary codes $C_3(1,n)$. In this paper, we describe a new class of $[2^n, n+1]$ ternary codes and a class of $[2^n, n+2]$ ternary codes, and determine their weight distributions. The supports of the minimum weight codewords of these codes give 1-designs under certain conditions. The supports of all codewords of some other weight also give 1-designs. As by-products, we present here four classes of 1-designs that are based on the ternary codes.

The purpose of this paper is to construct a class of $[2^n, n+2, 2^{n-1}]$ ternary codes (see Proposition 13) to improve the ternary $[2^n, n+1, 2^{n-1}]$ codes $C_3(1,n)$ that are the

* Corresponding author.

E-mail addresses: dingcs@comp.nus.edu.sg (C. Ding), torleiv@ii.uib.no (T. Kløve), sica@comp.nus.edu.sg (F. Sica).

PII: S0166-218X(00)00343-7

analogue of the binary first-order Reed–Muller codes $\mathrm{RM}(1,n)$ and are described by Ding et al. [2].

2. The class of ternary codes $C_3(r, n)$

Note that $(\mathrm{GF}(2)^n, +)$ is an additive Abelian group of exponent 2 and order $N = 2^n$, with $\mathbf{0}$ as the identity element. From now on we assume that $n \geqslant 2$. Let M denote the multiplicative group of characters from $\mathrm{GF}(2)^n$ to $\mathrm{GF}(3)^*$. The group M is isomorphic noncanonically to $\mathrm{GF}(2)^n$ [10, Chapter VI]. In particular, we have $|M| = |\mathrm{GF}(2)^n| = N = 2^n$. The set $\mathrm{GF}(2)^n$ may be identified with the set of integers $\{i\colon 0 \leqslant i \leqslant 2^n - 1\}$: the element $(i_0, i_1, \ldots, i_{n-1})$ of $\mathrm{GF}(2)^n$ is identified with $i = i_0 + i_1 2 + \cdots + i_{n-1}2^{n-1}$, where each i_j is 0 or 1. We also say that $(i_0, i_1, \ldots, i_{n-1})$ is the binary representation of i. We define

$$f_i(y) = (-1)^{i_0 y_0 + i_1 y_1 + \cdots + i_{n-1} y_{n-1}}, \tag{1}$$

where $y = (y_0, y_1, \ldots, y_{n-1}) \in \mathrm{GF}(2)^n$, and $(i_0, i_1, \ldots, i_{n-1})$ is the binary representation of i. It is easy to check that, for all i with $0 \leqslant i \leqslant 2^n - 1$, this gives all the 2^n characters from $\mathrm{GF}(2)^n$ to $\mathrm{GF}(3)^*$ with f_0 as the trivial character, so $M = \{f_0, f_1, \ldots, f_{2^n-1}\}$. Since we identify i and y with their respective binary representation, we have $f_i(y) = f_y(i)$. For any subset X of $\mathrm{GF}(2)^n$, the group character code C_X over $\mathrm{GF}(3)$ described by Ding et al. [3] is

$$C_X = \left\{ (c_0, c_1, \ldots, c_{N-1}) \in \mathrm{GF}(3)^N\colon \sum_{i=0}^{N-1} c_i f_i(x) = 0 \text{ for all } x \in X \right\}.$$

Let $X = \{x_0, x_1, \ldots, x_{t-1}\}$ be a subset of $\mathrm{GF}(2)^n$ and let X^{c} be the complement of X in $\mathrm{GF}(2)^n$, indexed such that $\mathrm{GF}(2)^n = \{x_0, x_1, \ldots, x_{N-1}\}$.

Proposition 1 (Ding et al. [2]). *Let X be as above. For $0 \leqslant i \leqslant N-1$, let v_i denote the vector*

$$(f_0(x_i), f_1(x_i), \ldots, f_{N-1}(x_i)).$$

Then the set $\{v_0, v_1, \ldots, v_{N-1}\}$ is linearly independent. In particular,

$$H = [f_{j-1}(x_{i-1})]_{1 \leqslant i \leqslant t,\ 1 \leqslant j \leqslant N}$$

has rank t and is a parity check matrix of C_X,

$$G = [f_{j-1}(x_{t-1+i})]_{1 \leqslant i \leqslant N-t,\ 1 \leqslant j \leqslant N}$$

has rank $N - t$ and is a generator matrix for C_X, so C_X is an $[N, N-t]$ linear code over $\mathrm{GF}(3)$. *Moreover, H is a generator matrix for $C_{X^{\mathrm{c}}}$ and $C_X \oplus C_{X^{\mathrm{c}}} = \mathrm{GF}(3)^N$.*

The Hamming weight of a vector $\boldsymbol{a}$ of $\mathrm{GF}(2)^n$, denoted $\mathrm{wt}(\boldsymbol{a})$, is defined to be the number of its nonzero coordinates. For $-1 \leqslant r \leqslant n$, let $X(r,n) = \{\boldsymbol{a} \in \mathrm{GF}(2)^n\colon\ \mathrm{wt}(\boldsymbol{a}) > r\}$, and let $C_3(r,n)$ denote the code $C_{X(r,n)}$ over GF(3). For a word $\boldsymbol{c}=(c_0,\ldots,c_{2^n-1})$ in $\mathrm{GF}(3)^{2^n}$, let the support of $\boldsymbol{c}$ be defined as

$$\mathrm{Supp}(\boldsymbol{c})=\{i\colon 0\leqslant i<2^n,\ \text{and}\ c_i\neq 0\}.$$

By convention, we define the minimum distance of the zero code to be ∞, which we represent by any integer larger than the block length of the code.

Proposition 2 (Ding et al. [2]). *The following properties of the codes $C_3(r,n)$ are known*:
(A) *$C_3(r,n)$ is a $[2^n,\sum_{j=0}^{r}\binom{n}{j},2^{n-r}]$ ternary code.*
(B) *The minimum nonzero weight codewords generate $C_3(r,n)$.*
(C) *The dual code $C_3(r,n)^{\perp}$ is equivalent to $C_3(n-r-1,n)$.*

In the sequel, we define $\upsilon_0=(1,1,\ldots,1)\in\mathrm{GF}(3)^n$ and

$$\upsilon_i=(f_0(\boldsymbol{e}_i),f_1(\boldsymbol{e}_i),\ldots,f_{N-1}(\boldsymbol{e}_i))$$

for all $1\leqslant i\leqslant n$, where $\boldsymbol{e}_i$ is the vector of $\mathrm{GF}(2)^n$ whose ith coordinate is 1 and other coordinates are all zero.

Proposition 3 (Ding et al. [3]). *For any integer $1\leqslant m\leqslant n+1$, in the code $C_3(1,n)$ there are $\binom{n+1}{m}2^m$ codewords of the form $\sum_{j=0}^{m-1}a_j\upsilon_{i_j}$ which have the same Hamming weight*

$$w(m){:=}2^{n-m+1}\frac{2^m-(-1)^m}{3}, \tag{2}$$

where all $a_j\in\mathrm{GF}(3)^*$, and $0\leqslant i_0<i_1<\cdots<i_{m-1}\leqslant n$. The n weights $w(m)$ in (2) are pairwise distinct and satisfy

$$\begin{aligned}&w(2)<w(4)<w(6)<\cdots<w(2\lfloor n/2\rfloor)<w(2\lfloor(n-1)/2\rfloor+1)\\&\quad<w(2\lfloor(n-1)/2\rfloor-1)<\cdots<w(5)<w(3)<w(1).\end{aligned}$$

For a ternary $[N,K]$ code C, let $A_i=A_i(C)$, $i=0,1,\ldots,N$, be its weight distribution and let

$$A_C(x)=\sum_{i=0}^{N}A_i(C)x^i.$$

be its weight distribution function. Then $A_C(x)$ and $A_{C^\perp}(x)$ are related by the MacWilliams identity (see e.g. [8, p. 88])

$$\begin{aligned}A_{C^\perp}(x)&=\frac{1}{3^K}\sum_{i=0}^{N}A_i(C)(1-x)^i(1+2x)^{N-i}\\&=\frac{1}{3^K}(1+2x)^N A_C\left(\frac{1-x}{1+2x}\right).\end{aligned}\tag{3}$$

It follows from Proposition 3 that

$$A_{C_3(1,n)}(x) = 1 + \sum_{m=1}^{n+1} \binom{n+1}{m} 2^m x^{w(m)}.$$

Combining this with (3) we get $A_{C_3(1,n)^\perp}(x)$. The explicit expressions for $A_i(C_3(1,n)^\perp)$ are quite complicated in general. However, we get $A_i(C_3(1,n)^\perp) = 0$ for $1 \leqslant i \leqslant 3$ (as we should since the code has minimum distance 4 by Proposition 3) and

$$A_4(C_3(1,n)^\perp) = \frac{6^n - 2 \cdot 4^n + 2^n}{4}. \tag{4}$$

In the rest of this section, we prove some auxiliary results for later sections and present a class of new 1-designs. The following lemma is a well-known result, known as the orthogonality relations in character theory [9, Chapter VI, Proposition 4].

Lemma 4. *Let A' be a finite additive Abelian group of order N' and let M' be the group of characters of A'. For characters f, g in M' and elements x, y in A', we have*:

1. $$\sum_{x \in A'} f(x)g(x) = \begin{cases} N' & \text{if } f = g^{-1}, \\ 0 & \text{if } f \neq g^{-1}. \end{cases}$$

2. $$\sum_{f \in M'} f(x)f(y) = \begin{cases} N' & \text{if } x = -y, \\ 0 & \text{if } x \neq -y. \end{cases}$$

Define $\boldsymbol{e}_0$ to be the zero vector of $GF(2)^n$. For each i with $1 \leqslant i \leqslant n$, $\boldsymbol{e}_i$ is defined as before. Let $\boldsymbol{e}_{n+1}, \boldsymbol{e}_{n+2}, \ldots, \boldsymbol{e}_{2^n-1}$ denote the elements of $GF(2)^n \setminus \{\boldsymbol{e}_0, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ with any order.

Define

$$\upsilon_i = (f_0(\boldsymbol{e}_i), f_1(\boldsymbol{e}_i), \ldots, f_{N-1}(\boldsymbol{e}_i))$$

for all $0 \leqslant i \leqslant 2^n - 1$. By Lemma 4, the vectors $\upsilon_0, \upsilon_1, \ldots, \upsilon_{2^n-1}$ are linearly independent over GF(3). Take any $n+1$ vectors $\upsilon_{j_0}, \upsilon_{j_1}, \ldots, \upsilon_{j_n}$, where $0 \leqslant j_0 < j_1 < \cdots < j_n \leqslant 2^n - 1$, we use $T_{j_0, j_1, \ldots, j_n}$ to denote the ternary code generated by $\upsilon_{j_0}, \upsilon_{j_1}, \ldots, \upsilon_{j_n}$.

Proposition 5. *If $1 \leqslant j_1 < j_2 < \cdots < j_n \leqslant 2^n - 1$ and $\boldsymbol{e}_{j_1}, \boldsymbol{e}_{j_2}, \ldots, \boldsymbol{e}_{j_n}$ are linearly independent, then $T_{0,j_1,\ldots,j_n}$ is equivalent to $C_3(1,n)$ and has thus the same parameters and weight distribution as $C_3(1,n)$. That is, for any integer $1 \leqslant m \leqslant n+1$, in the code $T_{0,j_1,j_2,\ldots,j_n}$ there are $\binom{n+1}{m}2^m$ codewords of the form $\sum_{l=0}^{m-1} a_l \upsilon_{j_{i_l}}$ which have the same Hamming weight $w(m)$, where $1 \leqslant i_0 < i_1 < \cdots < i_{m-1} \leqslant n$.*

Proof. Note that $C_3(1,n) = T_{0,1,\ldots,n}$. To prove the equivalence, we will show that by some column permutations a generator matrix of $T_{0,j_1,\ldots,j_n}$ gives a generator matrix of $T_{0,1,\ldots,n}$.

Consider the following matrices:

$$M(j_1,\dots,j_n):=[\boldsymbol{e}_l\boldsymbol{e}_{j_i}]_{1\leqslant i\leqslant n, 0\leqslant l\leqslant 2^n-1}$$

and

$$G(j_1,\dots,j_n):=[(-1)^{\boldsymbol{e}_l\boldsymbol{e}_{j_i}}]_{0\leqslant i\leqslant n, 0\leqslant l\leqslant 2^n-1},$$

where $e_{j_1}, e_{j_2}, \dots, e_{j_n}$ are linearly independent, and $\boldsymbol{e}_0\boldsymbol{e}_{j_1}$ denotes the standard inner product. Since $\boldsymbol{e}_{j_1}, \boldsymbol{e}_{j_2}, \dots, \boldsymbol{e}_{j_n}$ are linearly independent over GF(2), every vector of GF$(2)^n$ appears exactly once as column vectors of the matrix $M(j_1,\dots,j_n)$. Hence, by some column permutations, $M(j_1,\dots,j_n)$ can be rearranged into $M(1,\dots,n)$. Therefore, the generate matrix $G(j_1,\dots,j_n)$ of $T_{0,j_1,\dots,j_n}$ can be rearranged into the generator matrix $G(1,\dots,n)$ of $T_{0,1,\dots,n}$ by the same column permutations. This proves the equivalence. □

Example 1. Consider the case $n=3$. We take $\boldsymbol{e}_{j_1}=(1,0,0)$, $\boldsymbol{e}_{j_2}=(0,1,0)$, and $\boldsymbol{e}_{j_3}=(1,1,1)$. The three vectors are linearly independent. Then the code T_{0,j_1,j_2,j_3} has parameters $[7,3,3]$ and generator matrix

$$\begin{bmatrix} 1&1&1&1&1&1&1&1\\ 1&2&1&1&2&2&1&2\\ 1&1&2&1&2&1&2&2\\ 1&2&2&2&1&1&1&2 \end{bmatrix}.$$

The weight enumerator of this code is $1+24x^4+16x^5+32x^6+8x^8$. This code is one of the best possible codes of this length and dimension.

Remark. The condition that $\boldsymbol{e}_{j_1}, \boldsymbol{e}_{j_2}, \dots, \boldsymbol{e}_{j_n}$ are linearly independent in Proposition 5 is necessary to ensure that the minimum weight of the code $T_{0,j_1,\dots,j_n}$ is 2^{n-1}. For example, in the case $n=3$ if we take $\boldsymbol{e}_{j_1}=(0,1,0)$, $\boldsymbol{e}_{j_2}=(0,0,1)$, and $\boldsymbol{e}_{j_3}=(0,1,1)$. The three vectors are linearly dependent. Then the code T_{0,j_1,j_2,j_3} has parameters $[7,3,1]$ and generator matrix

$$\begin{bmatrix} 1&1&1&1&1&1&1&1\\ 1&1&2&1&2&1&2&2\\ 1&1&1&2&1&2&2&2\\ 1&1&2&2&2&2&1&1 \end{bmatrix}.$$

The weight enumerator of this code is $1+8x^2+24x^4+32x^6+16x^8$. So the minimum distance is less than 2^{n-1}.

Proposition 6. *The set of supports of the minimum nonzero weight codewords of $T_{0,j_1,j_2,\dots,j_n}$ in Proposition 5 is a $1-(2^n, 2^{n-1}, n(n+1)/2)$ design.*

Proof. This can be proved similarly as Corollary 17 in [2]. □

It is interesting to note that the code $T_{0,j_1,j_2,\dots,j_n}$ in Proposition 5 has only one odd weight $w(n+1)$. Only codewords of form $\sum_{i=0}^{n} a_i v_i$ have this odd weight, where each $a_i \neq 0$. We now prove that the supports of these codewords give 1-designs.

First, we quote an old result of C. Ramus from 1834 which will be needed in the proof and also later.

Lemma 7 (Knuth [8, p. 70]). *Let m and μ be positive integers and $0 \leqslant i < \mu$. Then*

$$\Delta_{\mu,i}(m) \stackrel{\text{def}}{=} \sum_{\substack{0 \leqslant j \leqslant m \\ j \equiv i \bmod \mu}} \binom{m}{j} = \frac{1}{\mu} \sum_{l=0}^{\mu-1} \left(2\cos\frac{l\pi}{\mu}\right)^m \cos\frac{l(m-2i)\pi}{\mu}.$$

Proposition 8. *The set of supports of all the codewords $\sum_{i=0}^{n} a_i v_i$, where each $a_i \neq 0$, in the code $T_{0,j_1,j_2,\dots,j_n}$ of Proposition 5, is a 1-$(2^n, (2^{n+1}-(-1)^{n+1})/3, \lambda)$ design, where*

$$\lambda = \begin{cases} \dfrac{2^{n+1}+(-1)^{n/3}2}{3} & \text{if } n \equiv 0 \pmod 3, \\ \dfrac{2^{n+1}-(-1)^{(n-1)/3}}{3} & \text{if } n \equiv 1 \pmod 3, \\ \dfrac{2^{n+1}+(-1)^{(n-2)/3}}{3} & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Proof. A codeword covers another one if and only if the set of supports of the former contains that of the latter. We first prove that a codeword $\boldsymbol{x} := \sum_{i=0}^{n} a_i v_i$ covers another one $\boldsymbol{y} := \sum_{i=0}^{n} b_i v_i$ if and only if one is a nonzero multiple of the other, where each a_i and b_i are nonzero. We need only to prove one direction of this claim as the other is obvious.

Assume now that $\boldsymbol{x}$ covers $\boldsymbol{y}$. Then $\boldsymbol{x}$ covers both $\boldsymbol{x} \pm \boldsymbol{y}$. Let h denote the Hamming distance between $(a_0, \dots, a_n)$ and $(b_0, \dots, b_n)$. If $h = n+1$ or $h = 0$, then $\boldsymbol{x}$ is a multiple of $\boldsymbol{y}$. Suppose that $h \neq 0$ and $h \neq n+1$. Then $\boldsymbol{x} - \boldsymbol{y}$ is a linear combination of h vectors v_i and $\boldsymbol{x} + \boldsymbol{y}$ is a linear combination of $n-h$ vectors v_i. If n is odd, one of h and $n-h$ is odd. If h is odd, by Proposition 5 the weight of $\boldsymbol{x} - \boldsymbol{y}$ is larger than that of $\boldsymbol{x}$, so $\boldsymbol{x}$ cannot cover $\boldsymbol{x} - \boldsymbol{y}$. If h is even, then $\boldsymbol{x}$ cannot cover $\boldsymbol{x} + \boldsymbol{y}$. If n is even, similarly we can prove that $\boldsymbol{x}$ cannot cover at least one of $\boldsymbol{x} \pm \boldsymbol{y}$. This leads to a contradiction. So h must be equal to one of 0 and $n+1$ and $\boldsymbol{x}$ must be a nonzero multiple of $\boldsymbol{y}$.

Hence, all the codewords of the form $\sum_{i=0}^{n} a_i v_i$, where $a_0 = 1$, give 2^n different supports. The weight of such a codeword is $w(n+1) = (2^{n+1} - (-1)^{n+1})/3$. We now consider the function $F_{d_1,\dots,d_n}(x) := 1 + d_1x_1 + d_2x_2 + \cdots + d_nx_n$ from $(\mathrm{GF}(3)^*)^n$ to $\mathrm{GF}(3)$, where each d_i is a nonzero element of $\mathrm{GF}(3)$ and $x = (x_1, \dots, x_n)$. The weight of $F_{d_1,\dots,d_n}(x)$ is defined to be the number of nonzero elements of $\mathrm{GF}(3)$ this function takes on when x ranges over all elements of $(\mathrm{GF}(3)^*)^n$. Since each d_i and x_i can be written in the form $(-1)^y$, where $y \in \mathrm{GF}(2)$, the weight of $F_{d_1,\dots,d_n}(x)$ does not depend on d_i. It then follows from the definition of these v_i that the set of supports of all

Table 1
Weight distribution of $T_{1,2,\dots,n,2^n-1}$ when n is even

Weight	Frequency	Codewords
$w(m)$, where $1 \leqslant m \leqslant n$	$\binom{n+1}{m}2^m$	$\sum_{l=0}^{m-1} a_l v_{j_l}$, where $j_l \in \{1,\dots,n,2^n-1\}$,
$\frac{2^{n+1}+1}{3}$	2^{n+1}	$\sum_{i=1}^{n} a_i v_i + a v_{2^n-1}$, $a_i \neq 0$, $a \neq 0$

these codewords is a 1-$(2^n, w(n+1), \lambda)$ design. It remains to determine λ. To this end, we need to consider the weight of $F_{1,\dots,1}(x)$. It is seen that the weight of this function is

$$2^n - |\{z \in \mathrm{GF}(2)^n\colon\ \mathrm{wt}(z) \equiv 2n-1 \pmod 3\}| = 2^n - \Delta_{3,i}(n),$$

where $i \equiv 2n-1 \pmod 3$. Then the λ, which is the weight of the function $F_{1,\dots,1}(x)$, is given by Lemma 7. This completes the proof of this proposition. □

3. Another class of $[2^n, n+1]$ ternary codes

Let e_{2^n-1} denote the all-one vector $(1,1,\dots,1)$ of $\mathrm{GF}(2)^n$, and let

$$v_{2^n-1} = (f_0(e_{2^n-1}), f_1(e_{2^n-1}), \dots, f_{2^n-1}(e_{2^n-1})).$$

Let $e_1, e_2, \dots, e_n$ be the n vectors as before. We use $T_{1,2,\dots,n,2^n-1}$ to denote the linear code generated by $v_1, v_2, \dots, v_n$ and v_{2^n-1}. By Lemma 4, $T_{1,2,\dots,n,2^n-1}$ has dimension $n+1$. We now determine the minimum weight and the weight distribution of this code.

Proposition 9. *The code* $T_{1,2,\dots,n,2^n-1}$ is a $[2^n, n+1, d]$ *ternary code, where d is given below.*

If n is even, then the minimum weight d of this code is 2^{n-1}, *and the weight distribution of this code is given in Table 1.*

If n is odd, then the minimum weight d of this code is

$$\min\{2^{n-1}, [2^{n+1} - 1 - 3^{(n+1)/2}]/3\},$$

and the weight distribution of this code is given in Table 2.

Case I: Since $\boldsymbol{u}$ and $a\boldsymbol{u}$ have the same Hamming weight if $a \neq 0$, we consider the weight of the following codeword:

$$\boldsymbol{u} := \sum_{l=0}^{m-2} a_l v_{j_l} + v_{2^n-1}, \tag{5}$$

where $j_l \in \{1,2,\dots,n\}$, $m-1 \leqslant n$, and each $a_l \neq 0$.

Table 2
Weight distribution of $T_{1,2,\dots,n,2^n-1}$ when n is odd

Weight	Frequency	Codewords
$w(m)$, where $1 \leqslant m \leqslant n$	$\binom{n+1}{m}2^m$	$\sum_{l=0}^{m-1} a_l v_{j_l}$, where $j_l \in \{1,\dots,n,2^n-1\}$,
$\frac{2^{n+1}-1-(-3)^{(n+1)/2}}{3}$	2^n	$\sum_{i=1}^{n} a_i v_i + a v_{2^n-1}$, where wt($\boldsymbol{h}$) even, $a_i \neq 0$, $a \neq 0$
$\frac{2^{n+1}-1+(-3)^{(n+1)/2}}{3}$	2^n	$\sum_{i=1}^{n} a_i v_i + a v_{2^n-1}$, where wt($\boldsymbol{h}$) odd, $a_i \neq 0$, $a \neq 0$

Subcase I.1: We consider the vector $\boldsymbol{u}$ of (5) under the condition that $m-1<n$. Each $a_l = (-1)^{h_l}$, where $h_l = \{0,1\}$. We now consider the following matrix:

$$L := \begin{bmatrix} \boldsymbol{e}_0\boldsymbol{e}_{j_0} + h_0 & \boldsymbol{e}_1\boldsymbol{e}_{j_0} + h_0 & \dots & \boldsymbol{e}_{2^n-1}\boldsymbol{e}_{j_0} + h_0 \\ \boldsymbol{e}_0\boldsymbol{e}_{j_1} + h_1 & \boldsymbol{e}_1\boldsymbol{e}_{j_1} + h_1 & \dots & \boldsymbol{e}_{2^n-1}\boldsymbol{e}_{j_1} + h_1 \\ \vdots & \vdots & & \vdots \\ \boldsymbol{e}_0\boldsymbol{e}_{j_{m-2}} + h_{m-2} & \boldsymbol{e}_1\boldsymbol{e}_{j_{m-2}} + h_{m-2} & \dots & \boldsymbol{e}_{2^n-1}\boldsymbol{e}_{j_{m-2}} + h_{m-2} \end{bmatrix}.$$

Since $\boldsymbol{e}_{j_0}, \boldsymbol{e}_{j_1}, \dots, \boldsymbol{e}_{j_{m-2}}$ are linearly independent, each vector of $\mathrm{GF}(2)^{m-1}$ appears exactly $2^{n-(m-1)}$ times as column vectors of L.

Let $j_{m-1}, j_m, \dots, j_{n-1}$ be the elements of $\{1,2,\dots,n\} \setminus \{j_0, j_1, \dots, j_{m-2}\}$. Consider now the following matrix:

$$L_1 := \begin{bmatrix} \boldsymbol{e}_0\boldsymbol{e}_{j_0} + h_0 & \boldsymbol{e}_1\boldsymbol{e}_{j_0} + h_0 & \dots & \boldsymbol{e}_{2^n-1}\boldsymbol{e}_{j_0} + h_0 \\ \boldsymbol{e}_0\boldsymbol{e}_{j_1} + h_1 & \boldsymbol{e}_1\boldsymbol{e}_{j_1} + h_1 & \dots & \boldsymbol{e}_{2^n-1}\boldsymbol{e}_{j_1} + h_1 \\ \vdots & \vdots & & \vdots \\ \boldsymbol{e}_0\boldsymbol{e}_{j_{m-2}} + h_{m-2} & \boldsymbol{e}_1\boldsymbol{e}_{j_{m-2}} + h_{m-2} & \dots & \boldsymbol{e}_{2^n-1}\boldsymbol{e}_{j_{m-2}} + h_{m-2} \\ \boldsymbol{e}_0\boldsymbol{e}_{j_{m-1}} & \boldsymbol{e}_1\boldsymbol{e}_{j_{m-1}} & \dots & \boldsymbol{e}_{2^n-1}\boldsymbol{e}_{j_{m-1}} \\ \vdots & \vdots & & \vdots \\ \boldsymbol{e}_0\boldsymbol{e}_{j_{n-1}} & \boldsymbol{e}_1\boldsymbol{e}_{j_{n-1}} & \dots & \boldsymbol{e}_{2^n-1}\boldsymbol{e}_{j_{n-1}} \end{bmatrix}.$$

Since $\boldsymbol{e}_{j_0}, \boldsymbol{e}_{j_1}, \dots, \boldsymbol{e}_{j_{n-1}}$ are linearly independent, each vector of $\mathrm{GF}(2)^{m-1}$ appears exactly once as a column vector of L_1.

Let $\boldsymbol{s}_0, \boldsymbol{s}_1, \dots, \boldsymbol{s}_{2^{m-1}-1}$ be all the vectors of $\mathrm{GF}(2)^{m-1}$, and we let $\boldsymbol{t}_0, \boldsymbol{t}_1, \dots, \boldsymbol{t}_{2^{n-(m-1)}-1}$ be all the vectors of $\mathrm{GF}(2)^{n-(m-1)}$. By permutations on columns, L_1 can be rearranged into the following matrix L_2:

$$\begin{bmatrix} \boldsymbol{s}_0 & \boldsymbol{s}_1 & \cdots & \boldsymbol{s}_{2^{m-1}-1} & \cdots & \boldsymbol{s}_0 & \boldsymbol{s}_1 & \cdots & \boldsymbol{s}_{2^{m-1}-1} \\ \boldsymbol{t}_0 & \boldsymbol{t}_0 & \cdots & \boldsymbol{t}_0 & \cdots & \boldsymbol{t}_{2^{n-(m-1)}-1} & \boldsymbol{t}_{2^{n-(m-1)}-1} & \cdots & \boldsymbol{t}_{2^{n-(m-1)}-1} \end{bmatrix}.$$

The weight of the codeword $\boldsymbol{u}$ in (5) can be determined by looking at the first $m-1$ rows of the matrix L_2. However, all the vectors $\boldsymbol{s}_i$ and $\boldsymbol{t}_i$ are needed to determine

Table 3
Distribution of elements of GF(3) in $\boldsymbol{u}$, where $g := (m-1-2w) \bmod 3$

$w := \mathrm{wt}(\boldsymbol{y})$	g	Entries of $\boldsymbol{u}$ when $\mathrm{wt}(x)$ even	Entries of $\boldsymbol{u}$ when $\mathrm{wt}(x)$ odd	Frequency
$w \equiv 0 \pmod 6$	$r-1$	r	$r-2$	$2^{n-m}\Delta_{6,0}(m-1)$
$w \equiv 1 \pmod 6$	r	$r-1$	$r-2$	$2^{n-m}\Delta_{6,1}(m-1)$
$w \equiv 2 \pmod 6$	$r-2$	$r-1$	r	$2^{n-m}\Delta_{6,2}(m-1)$
$w \equiv 3 \pmod 6$	$r-1$	$r-2$	r	$2^{n-m}\Delta_{6,3}(m-1)$
$w \equiv 4 \pmod 6$	r	$r-2$	$r-1$	$2^{n-m}\Delta_{6,4}(m-1)$
$w \equiv 5 \pmod 6$	$r-2$	r	$r-1$	$2^{n-m}\Delta_{6,5}(m-1)$

Table 4
The frequency distribution of the elements of GF(3) in $\boldsymbol{u}$

	r	$r-1$	$r-2$
$m-1=3k$	$\frac{2^m+(-1)^k}{3}2^{n-m}$	$\frac{2^m-(-1)^k2}{3}2^{n-m}$	$\frac{2^m+(-1)^k}{3}2^{n-m}$
$m-1=3k+1$	$\frac{2^m-(-1)^k}{3}2^{n-m}$	$\frac{2^m-(-1)^k}{3}2^{n-m}$	$\frac{2^m+(-1)^k2}{3}2^{n-m}$
$m-1=3k+2$	$\frac{2^m-(-1)^k2}{3}2^{n-m}$	$\frac{2^m+(-1)^k}{3}2^{n-m}$	$\frac{2^m+(-1)^k}{3}2^{n-m}$

the corresponding coordinates of v_{2^n-1}. This is because by definition $f_x(\boldsymbol{e}_{2^n-1}) = (-1)^{x_0+x_1+\cdots+x_{n-1}}$, where $(x_0, x_1, \ldots, x_{n-1})$ is the binary representation of the integer x.

Define $r = m \bmod 3$. We use $\boldsymbol{y}$ to denote one of the vectors $\boldsymbol{s}_i$ and $\boldsymbol{x}$ to denote one of the vectors $\boldsymbol{t}_i$. Then $(\boldsymbol{y}^{\mathrm{T}}, \boldsymbol{x}^{\mathrm{T}})^{\mathrm{T}}$ ranges over all column vectors of L_2 when $\boldsymbol{y}$ and $\boldsymbol{x}$ run over all vectors of $\mathrm{GF}(2)^{m-1}$ and $\mathrm{GF}(2)^{n-(m-1)}$, respectively, where $\boldsymbol{y}^{\mathrm{T}}$ denotes the transpose of $\boldsymbol{y}$. Let w be the Hamming weight of $\boldsymbol{y}$. Suppose that $\boldsymbol{y}$ and $\boldsymbol{x}$ are in the ith column of L_2, then $(m-1-2w) \bmod 3$ is the corresponding entry of the codeword $\sum_{l=0}^{m-2} a_l v_{j_l}$, and $(m-1-2w+(-1)^{w+\mathrm{wt}(\boldsymbol{x})}) \bmod 3$ is the corresponding entry of the codeword $\sum_{l=0}^{m-2} a_l v_{j_l} + v_{2^n-1}$. It is then seen that Table 3 gives the distribution of the elements $\{r, r-1, r-2\}$ of GF(3) in the codeword $\boldsymbol{u}$ of (5).

By Table 3, we have the following frequency of appearance of the elements of GF(3) in the codeword $\boldsymbol{u}$, where $r \in \mathrm{GF}(3)$:

$$\begin{array}{ll}
r & \text{Frequency} \\
\hline
r & [\Delta_{6,0}(m-1)+\Delta_{6,5}(m-1)+\Delta_{6,2}(m-1)+\Delta_{6,3}(m-1)]2^{n-m} \\
r-1 & [\Delta_{6,1}(m-1)+\Delta_{6,2}(m-1)+\Delta_{6,4}(m-1)+\Delta_{6,5}(m-1)]2^{n-m} \\
r-2 & [\Delta_{6,3}(m-1)+\Delta_{6,4}(m-1)+\Delta_{6,0}(m-1)+\Delta_{6,1}(m-1)]2^{n-m}
\end{array} \tag{6}$$

By Lemma 7 and (6), the frequency of appearance of the elements of GF(3) in the codeword $\boldsymbol{u}$ is given in Table 4.

Table 5
The weight of $\boldsymbol{u}$ in Subcase I.2

	wt($\boldsymbol{u}$) (wt($\boldsymbol{h}$) even)	wt($\boldsymbol{u}$) (wt($\boldsymbol{h}$) odd)
n even	$\frac{2^{n+1}+1}{3}$	$\frac{2^{n+1}+1}{3}$
n odd	$\frac{2^{n+1}-1-(-3)^{(n+1)/2}}{3}$	$\frac{2^{n+1}-1+(-3)^{(n+1)/2}}{3}$

With Table 4, we obtain that

$$\mathrm{wt}(\boldsymbol{u}) = \begin{cases} \frac{2^{m+1}+(-1)^k 2}{3} 2^{n-m} & \text{if } m-1=3k, \\ \frac{2^{m+1}-(-1)^k 2}{3} 2^{n-m} & \text{if } m-1=3k+1, \\ \frac{2^{m+1}+(-1)^k 2}{3} 2^{n-m} & \text{if } m-1=3k+2. \end{cases}$$

It is then easy to check that $\mathrm{wt}(\boldsymbol{u}) = w(m)$.

Subcase I.2: We consider the codeword $\boldsymbol{u}$ of (5) under the condition that $m-1=n$. Let $a_l = (-1)^{h_l}$, where $h_l \in \{0,1\}$. Define $\boldsymbol{h} = (h_0, h_1, \ldots, h_{m-2})$. To determine the weight of $\boldsymbol{u}$, we need the values of some $\Delta_{6,i}(n) + \Delta_{6,j}(n)$ given in Lemma 7. With an argument similar to that in Subcase I.1, we obtain the weight of $\boldsymbol{u}$ given in Table 5.

Case II: For any codeword

$$\boldsymbol{u} := \sum_{l=0}^{m-1} a_l v_{j_l}, \tag{7}$$

where $j_l \in \{1, 2, \ldots, n\}$, the weight of $\boldsymbol{u}$ is $w(m)$ as described in Proposition 5.

Summarizing the discussion in the two cases proves the conclusion of this proposition. □

Lemma 10. *If* $n \geqslant 13$ *and* n *is odd*, *then*

$$2^{n-1} < [2^{n+1} - 1 - 3^{(n+1)/2}]/3.$$

If $n \geqslant 8$ *and* n *is even*, *then*

$$2^{n-1} < [2^{n+2} - 1 - 3^{(n+2)/2}]/6.$$

Proof. The two inequalities can be easily proved by induction on n. □

Remark. If n is even, then $A_{T_{1,2,\ldots,n,2^n-1}}(x) = A_{C_3(1,n)}(x)$. In particular, the minimum weight of the code $T_{1,2,\ldots,n,2^n-1}$ is 2^{n-1} and the minimum weight of the dual code is 4.

When n is odd, the minimum weight of the code $T_{1,2,\ldots,n,2^n-1}$ is

$$d = \min\{2^{n-1}, [2^{n+1} - 1 - 3^{(n+1)/2}]/3\} = \begin{cases} < 2^{n-1} & \text{if } n \leqslant 11, \\ = 2^{n-1} & \text{if } n \geqslant 13. \end{cases}$$

Using MacWilliams identity, we get

$$A_1(T^{\perp}_{1,2,\ldots,n,2^n-1}) = 0,$$
$$A_2(T^{\perp}_{1,2,\ldots,n,2^n-1}) = 2^n.$$

In particular, the minimum weight of the dual code is 2.

Proposition 11. *If n is even or if $n \geqslant 13$ is odd, then the minimum weight codewords of $T_{1,2,\ldots,n,2^n-1}$ generate this code.*

Proof. By Proposition 9 and Lemma 10, in both cases the minimum weight codewords are of the form $av_i + bv_j$, where $i < j$. Thus, it suffices to prove that $v_{2^n-1} + v_{j_1}$, $v_{2^n-1} + v_{j_2}, \ldots, v_{2^n-1} + v_{j_n}$, and $v_{2^n-1} - v_{j_n}$ are linearly independent. This can be easily proved as v_{2^n-1}, v_0, v_1, $\ldots$, v_n are linearly independent. □

Proposition 12. *The set of supports of the minimum nonzero weight codewords of $T_{1,2,\ldots,n,2^n-1}$ is a 1-$(2^n, 2^{n-1}, n(n+1)/2)$ design when n is even or $n \geqslant 13$ is odd.*

Proof. Note that the minimum weight codewords of $T_{1,2,\ldots,n,2^n-1}$ must be of the form $av_i + bv_i$, where $i \neq j$, $a \neq 0$, and $b \neq 0$, when n is even or $n \geqslant 13$ is odd. This proposition can then be proved similarly as Corollary 17 in [2]. □

Example 2. Consider the case $n = 4$. We take $\boldsymbol{e}_{j_i} = \boldsymbol{e}_i$ for $i = 1, 2, 3, 4$. The four vectors are linearly independent. Then the code $T_{j_1,j_2,j_3,j_4,2^4-1}$ has parameters $[4, 7]$ and generator matrix

$$\begin{bmatrix} 1&2&1&1&1&2&2&2&1&1&1&2&2&2&1&2 \\ 1&1&2&1&1&2&1&1&2&2&1&2&2&1&2&2 \\ 1&1&1&2&1&1&2&1&2&1&2&2&1&2&2&2 \\ 1&1&1&1&2&1&1&2&1&2&2&1&2&2&2&2 \\ 1&2&2&2&2&1&1&1&1&1&1&2&2&2&2&1 \end{bmatrix}.$$

The weight enumerator of this code is $1 + 40x^8 + 80x^{10} + 32x^{11} + 80x^{12} + 10x^{16}$. The best ternary codes of length 16 and dimension 5 have minimum distance 9. So this is almost the best code of these parameters.

4. A class of $[2^n, n+2]$ ternary codes

Let $T_{0,1,2,\ldots,n,2^n-1}$ denote the code generated by v_0, v_1, $\ldots$, v_n and v_{2^n-1}. Clearly, it has dimension $n+2$. The minimum distance and weight distribution of this code is given in the following proposition.

Proposition 13. *The code $T_{0,1,2,\ldots,n,2^n-1}$ is a $[2^n, n+2, d]$ ternary code, where d is given below.*

Table 6
Weight distribution of $T_{0,1,2,\cdots,n,2^n-1}$ when n is even, where all a_i and a are nonzero.

Weight	Frequency	Codewords
$w(m)$, where $1 \leqslant m \leqslant n$	$\binom{n+2}{m}2^m$	$\sum_{l=0}^{m-1} a_l v_{j_l}$, where $j_l \in \{0,1,\ldots,n,2^n-1\}$,
$w(n+1)$	$(n+1)2^{n+1}$	$\sum_{l=0}^{n} a_l v_{j_l}$, where $j_0 = 0,\ j_l \in \{0,1,\ldots,n,2^n-1\}$
$\frac{2^{n+1}+1}{3}$	2^{n+1}	$\sum_{i=1}^{n} a_i v_i + a v_{2^n-1}$
$\frac{2^{n+2}-1+3(-3)^{n/2}}{6}$	2^{n+1}	$\sum_{l=0}^{n} a_l v_l + a v_{2^n-1}$
$\frac{2^{n+2}-1-3(-3)^{n/2}}{6}$	2^{n+1}	$\sum_{l=0}^{n} a_l v_l + a v_{2^n-1}$

Table 7
Weight distribution of $T_{0,1,2,\ldots,n,2^n-1}$ when n is odd, where all a_l and a are nonzero

Weight	Frequency	Codewords
$w(m)$, where $1 \leqslant m \leqslant n$	$\binom{n+2}{m}2^m$	$\sum_{l=0}^{m-1} a_l v_{j_l}$, where $j_l \in \{0,1,\ldots,n,2^n-1\}$,
$w(n+1)$	$(n+1)2^{n+1}$	$\sum_{l=0}^{n} a_l v_{j_l}$, where $j_0 = 0,\ j_l \in \{0,1,\ldots,n,2^n-1\}$
$\frac{2^{n+1}-1-(-3)^{(n+1)/2}}{3}$	2^n	$\sum_{i=1}^{n} a_i v_i + a v_{2^n-1}$
$\frac{2^{n+1}-1+(-3)^{(n+1)/2}}{3}$	2^n	$\sum_{i=1}^{n} a_i v_i + a v_{2^n-1}$
$\frac{2^{n+2}+1+(-3)^{(n+1)/2}}{6}$	2^{n+1}	$\sum_{l=0}^{n} a_l v_l + a v_{2^n-1}$
$\frac{2^{n+2}+1-(-3)^{(n+1)/2}}{6}$	2^{n+1}	$\sum_{l=0}^{n} a_l v_l + a v_{2^n-1}$

If n is even, then the minimum weight d of this code is

$$\min\{2^{n-1}, \tfrac{1}{6}[2^{n+2} - 1 - (3)^{(n+2)/2}]\}$$

and the weight distribution of this code is given in Table 6.

If n is odd, then the minimum weight d of this code is

$$\min\{2^{n-1}, (2^{n+1} - 1 - 3^{(n+1)/2})/3\},$$

and the weight distribution of this code is given in Table 7.

Proof. Note that $T_{0,1,2,\ldots,n,2^n-1}$ contains both $T_{0,1,2,\ldots,n}$ and $T_{1,2,\ldots,n,2^n-1}$ as subcodes. We need only to consider the codewords

$$\boldsymbol{u} := a_0 v_0 + \sum_{l=1}^{m-2} a_l v_l + a v_{2^n-1},$$

where $a_l \neq 0$ and $a \neq 0$. If $m-2 < n$, with an argument similar to Subcase I.1 of Section 3, we can prove that $\mathrm{wt}(\boldsymbol{u}) = w(m)$. If $m-2 = n$, similarly, we can prove the following:

(1) If n is even, $\mathrm{wt}(\boldsymbol{u})$ takes on $(2^{n+2}-1+3(-3)^{n/2})/6$ and $(2^{n+2}-1-3(-3)^{n/2})/6$, respectively for 2^{n+1} codewords $\boldsymbol{u}$.

(2) If n is odd, $\mathrm{wt}(\boldsymbol{u})$ takes on $(2^{n+2}+1+(-3)^{(n+1)/2})/6$ and $(2^{n+2}+1-(-3)^{(n+1)/2})/6$, respectively for 2^{n+1} codewords $\boldsymbol{u}$.

Combining these two conclusions and Propositions 5 and 9 proves this proposition. □

Remark. 1. Combining Proposition 13 and MacWilliams identity we get that the code $(T_{0,1,2,\dots,n,2^n-1})^{\perp}$ has minimum weight 4 and

$$A_4((T_{0,1,2,\dots,n,2^n-1})^{\perp}) = \begin{cases} (3\cdot 6^n - 8\cdot 4^n + 5\cdot 2^n)/16 & \text{if } n \text{ is even}, \\ (3\cdot 6^n - 8\cdot 4^n + 7\cdot 2^n)/16 & \text{if } n \text{ is odd}. \end{cases}$$

2. By Lemma 10, if $n \geqslant 8$ and n is even or if $n \geqslant 13$ and n is odd, $T_{0,1,2,\dots,n,2^n-1}$ has minimum distance $d = 2^{n-1}$. Thus the code $T_{0,1,2,\dots,n,2^n-1}$ is better than $T_{1,2,\dots,n,2^n-1}$ and $T_{0,1,2,\dots,n}$ except for a few n's.

Proposition 14. *If $n \geqslant 8$ is even or if $n \geqslant 13$ is odd, then the minimum weight codewords of $T_{0,1,2,\dots,n,2^n-1}$ generate this code.*

Proof. The proof of Proposition 11 applies here. □

Proposition 15. *The set of supports of the minimum nonzero weight codewords of $T_{0,1,2,\dots,n,2^n-1}$ is a 1-$(2^n, 2^{n-1}, (n+2)(n+1)/2)$ design when $n \geqslant 8$ is even or $n \geqslant 13$ is odd.*

Proof. Note that all the minimum weight codewords of $T_{0,1,2,\dots,n,2^n-1}$ must be of the form $av_i + bv_j$, where $i \neq j$, $a \neq 0$, and $b \neq 0$, when $n \geqslant 8$ is even or $n \geqslant 13$ is odd. Then this proposition can be proved similarly as Corollary 17 in [2]. □

5. Using the codes for error detection

Let C be a ternary $[N, K, d]$ code. The probability of undetected error when the code is used purely for error detection on a ternary symmetric channel is given by

$$P_{\mathrm{ue}}(C, p) = \sum_{i=d}^{N} A_i(C)\left(\frac{p}{2}\right)^i (1-p)^{N-i},$$

where p is the symbol error probability (see, e.g., Kløve and Korzhik [6]). In particular,

$$P_{\mathrm{ue}}(C, 2/3) = (3^K - 1)(1/3)^N < 3^{K-N}. \tag{8}$$

The error probability threshold of C, introduced in Kløve [5], is defined by

$$\theta(C) = \max\{p' \in [0, 2/3] \mid P_{ud}(C, p) \leqslant P_{ud}(C, 2/3) \text{ for all } p \in [0, p']\}.$$

A code C is called good for error detection (in the technical sense) if and only if $\theta(C) = 2/3$. However, for practical applications the important things are that $P_{\mathrm{ue}}(C, 2/3)$

is small (that is, $N-K$ is large) and that $\theta(C)$ is above the range of actual values of p. It is therefore of interest to estimate $\theta(C)$. It turns out that the performances on error detection of the codes described in this paper are very similar. Therefore, we will only discuss $C=C_3(1,n)$ in detail. For this code, we have $N=2^n$, $K=n+1$ and $d=2^{n-1}$.

Proposition 16. *For all $n\geqslant 2$ we have*

$$\frac{1}{3}<\theta(C_3(1,n))<\frac{1}{3}+\frac{n}{2^{n-2}}.$$

Proof. First, we note that for fixed $p\in(0,\frac{2}{3})$, the expression $(p/2(1-p))^i$ decreases with increasing i. Hence,

$$\begin{aligned} P_{\mathrm{ue}}(C,p) &= (1-p)^N\sum_{i=d}^{N} A_i(C)\left(\frac{p}{2(1-p)}\right)^i \\ &< (1-p)^N\sum_{i=d}^{N} A_i(C)\left(\frac{p}{2(1-p)}\right)^d \\ &= \left(\frac{p(1-p)}{2}\right)^{N/2}(3^K-1). \end{aligned}$$

Further, we note that $p(1-p)$ is increasing on the interval $(0,\frac{1}{2})$. Hence, if $p\leqslant\frac{1}{3}$, then

$$P_{\mathrm{ue}}(C,p)\leqslant P_{\mathrm{ue}}\left(C,\frac{1}{3}\right)<\left(\frac{1}{9}\right)^{N/2}(3^K-1)=\left(\frac{1}{3}\right)^{N}(3^K-1)=P_{\mathrm{ue}}\left(C,\frac{2}{3}\right).$$

Hence,

$$\theta(C)>\tfrac{1}{3}.$$

A direct calculation of $\theta(C)$ for $n\leqslant 9$ gives the following values:

n	2, 3, 4, 5	6	7	8	9
$\theta(C)$	$\frac{2}{3}$	0.4369	0.3852	0.3619	0.3427
$\frac{1}{3}+n/2^{n-3}$	$>\frac{2}{3}$	1.0833	0.7708	0.5833	0.3759

In particular, the upper bound is true for $n\leqslant 9$. To prove the upper bound for $n\geqslant 10$, we first note that $A_d(C)\geqslant 3$. Let p be the root in the interval $(0,\frac{1}{2})$ of the equation

$$\left(\frac{p(1-p)}{2}\right)^{2^{n-1}}=\frac{3^n}{3^{2^n}},$$

that is

$$p=\frac{3-\sqrt{9-8\cdot 3^{n/2^{n-1}}}}{6}.$$

Then

$$P_{\mathrm{ue}}(C,p) \geqslant A_d \left(\frac{p}{2}\right)^{2^{n-1}} (1-p)^{2^{n-1}}$$

$$> 3\left(\frac{p(1-p)}{2}\right)^{2^{n-1}}$$

$$= \frac{3^{n+1}}{3^{2^n}} > P_{\mathrm{ue}}(C,2/3).$$

Hence,

$$\theta(C) < p.$$

Simple calculus shows that

$$\frac{3-\sqrt{9-8x}}{6} < \frac{1}{3} + 4\log_3 x$$

for $1 < x < 1.12$. Hence,

$$p < \frac{1}{3} + \frac{n}{2^{n-3}}$$

for $n \geqslant 10$. □

Proposition 16 shows that $C_3(1,n)$ is good for practical error detection (even if it is not "good" in the technical sense). A similar proof shows that also the other codes have a threshold close to $\frac{1}{3}$ (for most n).

Now, consider the dual codes.

Proposition 17. *For all $n \geqslant 13$ we have*

$$\theta(C_3(1,n)^{\perp}) < \frac{6}{18^{n/4}}.$$

Proof. We have

$$P_{\mathrm{ue}}(C^{\perp},2/3) = \frac{3^{2^n-n-1}-1}{3^{2^n}} < \frac{1}{3^{n+1}}.$$

Let

$$p = \frac{6}{18^{n/4}}.$$

We have $p < \frac{2}{3}$ for $n \geqslant 4$. By (4), we have

$$\frac{P_{\mathrm{ue}}(C^{\perp},p)}{P_{\mathrm{ue}}(C^{\perp},2/3)} > A_4(C^{\perp})\left(\frac{p}{2}\right)^4 (1-p)^{2^n-4}\cdot 3^{n+1}$$

$$= \frac{243}{16}\left(1-2\left(\frac{2}{3}\right)^n + \left(\frac{1}{3}\right)\right)\left(1-\frac{6}{18^{n/4}}\right)^{2^n-4} > 1$$

for all $n \geqslant 13$. □

Proposition 17 shows that $C_3(1,n)^\perp$ is not very useful for error detection except possibly for some very moderate values of n. The upper bound on $\theta(C_3(1,n)^\perp)$ can be improved by some factor by the same method, e.g.

$$\theta(C_3(1,n)^\perp) < \frac{3}{18^{n/4}} \quad \text{for } n \geqslant 28.$$

However, it is of less interest to determine precise bounds on $\theta(C_3(1,n)^\perp)$ since it is very small in any case.

6. Concluding remarks

The code $T_{1,2,\ldots,n,2^n-1}$ cannot be equivalent to $T_{0,1,\ldots,n}$ when n is odd. This is because $T_{1,2,\ldots,n,2^n-1}$ has only even weights when n is odd, while $T_{0,1,\ldots,n}$ has always one odd weight $w(n+1)$. When $n \geqslant 13$, the minimum weight of $T_{1,2,\ldots,n,2^n-1}$ is still 2^{n-1}.

When $n \geqslant 8$ is even or $n \geqslant 13$ is odd, the ternary code $T_{0,1,2,\ldots,n,2^n-1}$ has length 2^n and minimum weight 2^{n-1}. But its dimension is $n+2$. So the codes $T_{0,1,2,\ldots,n,2^n-1}$ constructed here improves the $[2^n, n+1, 2^{n-1}]$ ternary codes described by Ding et al. [3].

The ternary codes $C_3(r,n)$ have the same parameters as the binary Reed–Muller codes $\mathrm{RM}(r,n)$. For binary Reed–Muller codes we have $\mathrm{RM}(r,n)^\perp = \mathrm{RM}(n-r-1,n)$. In analogue, $C_3(n-r-1,n)$ is the dual of $C_3(r,n)$ with respect to a twisted inner product $\langle \boldsymbol{u}, v\rangle = \sum_{i=0}^{2^n-1} a_j u_j v_j$, where the a_j's are some constants [2]. Another similarity is that the minimum weight codewords generate the codes. Thus, the ternary codes $C_3(r,n)$ may be viewed as the analogue of the binary Reed–Muller codes $\mathrm{RM}(r,n)$. However, there are differences between them. For example, the first-order Reed–Muller codes $\mathrm{RM}(1,n)$ are two-weight codes, while the ternary codes $C_3(1,n)$ have many weights (see Proposition 3). Some of these comments on the similarity and differences between $C_3(r,n)$ and $\mathrm{RM}(r,n)$ also apply to the class of ternary codes $T_{1,2,\ldots,n,2^n-1}$.

Finally, one of the referees pointed out that the weight distribution of the codes $C_3(1,n)$ described in Proposition 3 is given by the eigenvalues of the Hamming scheme, namely the number of codewords of weight $w(m)$ is the value of a Krawtchouk polynomial, that is $\binom{n+1}{m}2^m = P_m(0,n+1)$. It may be interesting to investigate the relationship between these codes and the Hamming scheme. Also it would be interesting to look at the automorphism group of the codes $C_3(r,n)$ and the two classes of ternary codes described in this paper.

Acknowledgements

The authors thank the two referees for their comments and suggestions that helped improve this paper.

References

[1] G.T. Bogdanova, I.G. Boukliev, New linear codes of dimension 5 over $GF(3)$, in: Proceedings of the fourth International Workshop on Algebraic and Combinatorial Coding Theory, 1994, pp. 41–43.

[2] C. Ding, D.R. Kohel, S. Ling, Elementary 2-group character codes, IEEE Trans. Inform. Theory 46 (2000) 280–284.

[3] C. Ding, D.R. Kohel, S. Ling, Secret sharing with a class of ternary codes, Theor. Comput. Sci. 246 (2000) 285–298.

[4] N. Hamada, T. Helleseth, Ø. Ytrehus, The nonexistence of $[51, 5, 33; 3]$-codes, Ars Combinat. 25 (1993) 25–32.

[5] T. Kløve, Reed–Muller codes for error detection, the good, the bad, and the ugly, IEEE Trans. Inform. Theory 42 (1996) 2265–2272.

[6] T. Kløve, V. Korzhik, Error Detecting Codes, General Theory and their Application in Feedback Communication Systems, Kluwer Academic Publishers, Boston, 1995.

[7] D.E. Knuth, The Art of Computer Programming, Vol. 1, 2nd Edition, Addison-Wesley, Reading, MA, 1973.

[8] V.S. Pless, W.C. Huffman, Handbook of Coding Theory, Vol. 1, North-Holland, Amsterdam, 1998.

[9] J.-P. Serre, A Course in Arithmetic, Graduate Texts in Mathematics, Vol. 7, Springer, New York, 1973.

[10] M. van Eupen, Four nonexistence results for ternary linear codes, IEEE Trans. Inform. Theory 41 (1995) 800–805.

[11] M. van Eupen, Some new results for ternary linear codes of dimension 5 and 6, IEEE Trans. Inform. Theory 41 (1995) 2048–2051.

[12] M. van Eupen, J.H. van Lint, On the minimum distance of ternary cyclic codes, IEEE Trans. Inform. Theory 39 (1993) 409–422.